USDA-APHIS-Wildlife Services
Privacy Impact Assessment

December 2007

Project Name:

Wildlife Services, Management Information System (MIS)

Description of Your Program/Project:

The Animal and Plant Health Inspection Service (APHIS), Wildlife Services (WS) Management Information System (MIS) was upgraded to a direct data, online-based system in FY 2005. The new system better serves the APHIS/WS program, its customers, and the public, by improving the program's capability to monitor and measure program performance; provide timely information to decision makers, and better document APHIS/WS activities.

MIS is especially important for record keeping of work in several areas of wildlife damage management related to agriculture, human health and safety, natural resources, and human property. These areas include, but are not limited to, wildlife diseases, airports, invasive species, livestock protection, blackbird damage management, and aquaculture protection. The MIS is the only data management system dedicated to tracking APHIS/WS activities and accomplishments nationwide. APHIS/WS has a strong interest in protecting the privacy of both its customers and employees as the new system is developed and maintained. To address privacy issues and to ensure protection of information provided by employees and customers, this Privacy Impact Assessment (PIA) has been developed.

MIS provides a state-of-the-art data tracking and management system. It provides computer access to all APHIS/WS employees nationwide for the first time in the history of the APHIS/WS program, and enables managers to have access to valuable data at the click of a button. It assists research by enabling operations personnel to gather data that in the past could not be collected. It provides APHIS/WS employees with the capability to generate specialized reports for their cooperators without the assistance of support personnel. It facilitates better information gathering and distribution, internally for decision makers and externally for all interested parties. Implementation of this system provides e-mail capability to all APHIS/WS employees enabling better and timelier communication with the workforce.

DEFINITIONS

MIS	Management Information System - the system in which APHIS/WS keeps data for which this PIA has been developed
Users	The collective group of individuals who have access to data in the system
Cooperative Agreement	An instrument generated by APHIS/WS which defines the financial arrangement, if any, the scope and focus of work to be performed, and mutually accepted terms of a wildlife damage management program between a customer and WS.
Customer	A public or private entity or individual who seeks and

	receives services from WS. These customers are referred to as “Cooperators” within WS, and in this document. A customer for whom WS does wildlife damage management or similar activities using WS employees to perform the work may be required to reimburse USDA under a funded Cooperative Service Agreement, whereas a customer who seeks and receives only technical advice participates in a part of the WS program that does not require reimbursement. Categories of customers include ranchers, farmers, livestock dealers, (including agents and brokers handling livestock covered by the program); airports, condominium associations, homeowner’s associations, golf courses, State, Federal, Tribal and Local Governments, pest control operators, homeowners, individuals, and contractual personnel engaged in program activities.
Work Initiation Document	Documents associated with permissions for WS to enter cooperator lands to perform work pursuant to wildlife damage management. Documents define species to be addressed, and methods, components or strategies to be used in the conduct of projects.

DATA IN THE SYSTEM

1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	**Customer (Cooperator) Data:** This is the minimal information kept by WS which is necessary for identifying cooperators for the purpose of communication with them, and tracking of activities performed by WS employees as part of a program being conducted in collaboration with them. This usually includes a name, telephone number, mailing address, physical location address, and for cooperators for whom WS provides staff to do work on specific wildlife damage management projects, an identifying number which may be a federal tax identification number, an employer identification number, or for individual citizens who are the primary contact in a funded cooperative agreement relationship, a social security number. A required identification number is only collected for those cooperators with whom APHIS/WS implements a funded agreement. Those cooperators who receive technical assistance consisting of written advice, on-site consultation, demonstrations of methods used, training, and similar free services are not required to provide such an identifier. Information about cooperators may also include resource and resource damage information. In some instances, GPS coordinates may be recorded for locations on properties where specific damage

	management actions, such as wildlife disease sampling or placing of some devices occur. **Employee data:** This is minimal and includes name, address and telephone number of duty station, user name, password and MIS specific employee identification number. **Other data:** This may be information related to adverse human or animal incidents, indemnity, agreements, or insurance claims. Additionally, information in the system may relate to resources owned by customers which was threatened, damaged or destroyed by wildlife.
2a. What are the sources of the information in the system?	Data is generated as a result of entries made about the work performed by WS Employees. Other data is collected by voluntary submission by customers. Basic look-up data is supplied from Integrated Taxonomic Information System (ITIS). WS purchases zip-code data from the postal service or another provider. Reference and lookup data about pesticide registration, wildlife laws and permits are obtained from Federal, State, and Local authorities.
2b. What USDA files and databases are used? What is the source agency?	USDA files are not applicable since MIS is program specific to its servers and databases. Source agency is APHIS/WS.
2c. What Federal Agencies are providing data for use in the system?	APHIS/WS. Reference data about pesticide registration and wildlife laws is obtained from Federal authorities and entered into the system by APHIS/WS data technicians. Information about permits granted to APHIS/WS for certain types of work is also in the system and is entered by APHIS/WS employees. In situations where the Federal Agency is the customer, as defined under #1 above, information concerning the Agency will be obtained and entered into the system.
2d. What State and Local Agencies are providing data for use in the system?	Reference data about pesticide registration and wildlife laws is obtained from State and Local authorities and entered into the system by APHIS/WS users. Information about permits granted to APHIS/WS for certain types of work is also entered into the system by APHIS/WS

	employees. In situations where the State or local Agency is the customer, as defined under #1 above, information concerning the Agency will be obtained and entered into the system.
2e. From what other third party sources will data be collected?	None.
2f. What information will be collected from the customer/employee?	**Customer:** name, address, phone number, customer identifying number, as applicable, and resources at risk. **Employee:** All Wildlife Services field activities.
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	Employees will sign off on "itinerary" reports verifying their work data was entered correctly. Customers will validate all information collected about themselves before it is entered into the system. Additionally, there is review by APHIS/WS supervisors and data specialists at the District, State, Regional and National levels.
3b. How will data be checked for completeness?	Signed paper forms containing data collected from customers (cooperators) will be checked by them at signature, by the APHIS/WS employee collecting the data, and at the office which originates the data before being "approved" in the system. Field work data will be checked for completeness by the APHIS/WS employee who enters it. This electronic data entry process is monitored by an internal validation prompt system built into the MIS. Data is again reviewed for accuracy by supervisors at the APHIS/WS District and State levels.

ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	Access to data in MIS is determined by the data usage role of the APHIS/WS employee which is determined by duties. Within the agency, access both as to limits and authority are compliant with APHIS “least privilege” rule (APHIS Directive 3140.5), for which policy is established further in APHIS/WS Directive 4.120 and detailed guidance is provided in the APHIS/WS Information and Data Management Handbook (IDMH) (2004). APHIS/WS employees authorized to access data at any level are collectively referred to in this document as **users**.

	Access to data in the system is limited to APHIS/WS personnel only and includes: APHIS/WS Deputy Administrator APHIS/WS System Owner and/or designees USDA-OCIO-National Information Technology Center APHIS/WS Information System Security Manager (ISSM) and / or designees APHIS/WS Information System Security Officer (ISSO) and / or designees APHIS/WS headquarters MIS liaison APHIS/WS data developers APHIS/WS system administrators APHIS/WS system manager APHIS/WS operational program managers APHIS/WS operational program data technicians APHIS/WS operational program field specialists APHIS/WS office administrative staff
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	Individual employees within APHIS/WS have limited access to some data based on their roles in the agency. A few individuals have access to all data, while most have limited access. Criteria and procedures, controls, and responsibilities regarding access are documented in APHIS/WS Directive 4.120 and the APHIS/WS Information and Data Management Handbook. Each user has his/her account, and password to the system. Accounts are given according to each state's individual policy. Within the system, each user has a specific role, determined at the State levels but codified and documented by the Working Group, as to how much data can be accessed. The different roles, such as User, District Supervisor, State Director, and Data Technician, are controlled by the database software (Oracle).
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	User access to data is restricted to data necessary for the user's job. The following describes the role and access of users of the MIS system of records: The **APHIS/WS Deputy Administrator (DA)** oversees the MIS System of Records as part of the total oversight of the APHIS/WS National Program. The role of this position is programmatic supervisor of the system owner. Data in the system will not be accessed by the DA directly, but through the system owner, the ISSM, a designated ISSO or the headquarters MIS liaison. The **System Owner**, who is the APHIS/WS Operational Support Staff Director, will work closely with ISSMs and

	ISSOs to ensure an effective ISS program. The role of the system owner is to provide supervisory oversight and administrative collaboration to the Information Technology Support Center (ITSC) management staff and provide input to the APHIS/WS Management Team regarding the MIS system of records. Duties also include oversight of the creation (or receipt), maintenance and use, and disposition of records in the system. The system owner will not access data directly, but through the ISSM, a designated ISSO, or the Headquarters MIS Liaison. Access by the system owner will be determined by a need to monitor or evaluate system integrity, efficiency, or general function, to evaluate various aspects of data handling or content, or to provide programmatic input about overall or component program activities with cooperators. **USDA's National Information Technology Center (NITC)**, administered by the USDA Office of the Chief Information Officer (OCIO) provides data management services to APHIS/WS for its MIS system of records. The OCIO's, assistants and/or designees who work at the NITC facility servicing APHIS/WS function as neutral users of APHIS/WS data. Their duties and responsibilities include handling of APHIS/WS data in accordance with standards established by NITC and APHIS/WS, continuous storage management, security administration, regular dataset backups, contingency planning/disaster recovery, and technical support. Access by individual employees at NITC is restricted to the need for implementing these actions, as assigned. NITC has established best management practices which include approved security measures for the protection of data of its clients. NITC managers collaborate with the APHIS/WS ISSM and her/his designees in handling and storage of APHIS/WS data. **The Information System Security Manager (ISSM) who** is also the Director of the APHIS/WS ITSC is appointed by the System Owner (Director of WS's Operational Support Staff), and is responsible for all security oversight of the electronic component of the MIS system of records. The ISSM appoints ISSOs and defines duties and security responsibilities for all APHIS/WS ITSC personnel who are users of the system. The ISSM collaborates with APHIS security experts and other APHIS/WS managers to develop security systems, protocol, and practices to protect the MIS system of records. The **Information System Security Officer(s) (ISSO)** are appointed or assigned ISSO duties by the ISSM and are responsible for ensuring that security measures are implemented and maintained within their area(s) of

	responsibility. Their duties include routine monitoring of MIS data entry, tabulation, storage, and retrieval within their areas of responsibility and providing prescribed reports in appropriate formats to the ISSM and other approved requesters. Access to data in the system is determined by the need of these officers to adequately monitor the use of the system within their purview. ISSOs may be granted access to the entire system of records by the ISSM for specific official duties necessitating this level of access. Access to data in the system by the headquarters **MIS liaison** is determined by the need for compiling reports or providing data related to operational and research program activities and accomplishments. The MIS liaison provides a diversity of reports and information to headquarters and operational and research managers about specific projects or their results on a state or national level. Verification of the accuracy of data about wildlife damage management or research activities for national reports comprising a compilation of all state reports is the responsibility of the MIS liaison. Only rarely will this individual require access to privacy information contained in the system, however. Access to data by **system administrators** is determined by the need to effectively perform tasks related to overall protection, troubleshooting, and modifications to programs and equipment that store the data. Although the administrator does not need access to view specific information about people in the database, duties do require access to all data in order to evaluate system integrity, efficiency, and function. The **system manager**, who is the MIS Working Group Chair, will participate in systems management by steering a working group in reviewing, updating, developing and maintaining policy and procedures for use of the system, collaborating with the MIS Center staff about system modifications, and acting as consultant to the APHIS/WS Management Team regarding MIS. Occasional access to data in the system is required in order to monitor quality of data entry and management. Access by **system developers** is based on the need to examine the nature of data being input and stored to determine formats and structures for capturing, storing and relating the data. Because improvements will be made to the system on an ongoing basis, input and output data will be available to system developers for stress testing and improving the overall function of the system and its software components.

	Access by **program managers** in APHIS/WS will be tiered based on the level of management occupied. District level managers of operational programs have access to all data related to their districts. State level managers have access to all data about their state operational program, while regional managers have access to data about their regional program. State, district, and regional managers also have access, through case-by-case approval by the state-level manager where specific data was collected, or by the headquarters MIS Liaison, for national level data, or to other state and national program information. **Operational program data technicians** will access data at the state program level for the purpose of providing reports upon request to various APHIS/WS managers, field employees, and other authorized requesters. Additionally, they will access their state's data in the system based on the need to assist in the process of error checking, validating, and consolidating data. Their access will be authorized by the incumbent State Director of the state-level program where they are employed. Operational program **field specialists'** access is determined by the needs demanded by role. This level of access is usually determined by the requirements for individual input of data generated when the employee records the results of work, by the need to validate input data, the need to provide information to cooperators about their projects, and the need to report to supervisors about details of work. Access of this nature is limited to viewing data input by the individual employee, and reports that are generated by the system. For special needs, the State Director may grant access to other data entered by other employees in the state. This access is read-only except where two or more specialists are working on one project and need to collaborate in the entry of data. Some **APHIS/WS office administrative staff** of district, state, regional, and national offices handle various data components. Most of these are hard copy documents for local file management. Access to the system for these staff members is limited to routine handling of such documents, except instances where the State Director authorizes data entry by these employees for specific purposes germane to state program goals. Some administrative personnel function as public contact specialists and provide information to requesters. They will collect information from such requesters and enter it into

	the system. They have access to only their input data for error checks and validation.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	Fundamental access control of the APHIS/WS information system is through unique identities and password authentication. These control tools are kept by the APHIS/WS ISSM and her/his designees, including ISSOs, and system administrators, and are created, activated, deactivated and managed by the ISSM and /or her/his designees. Restrictions on the amount and nature of data within the database which is made available to each user is determined and maintained through assignment of roles according to business rules set by the MIS Working Group, whose chairperson is the APHIS/WS system manager. Criteria and procedures for qualifying for specific information access levels are provided in APHIS/WS information technology policy guidelines. Control protocol is determined by the ISSM and is also documented in business rules and related system use policy and procedure. Access through these roles is governed within the system through a password protection protocol monitored, maintained, and updated by the ISSM and / or designees. Control measures which are designed to prevent misuse of accessible data include limitation of user roles through business rules and compartmentalization of allowed access. Users at APHIS/WS district, state, and regional levels are restricted to data according to the "least privilege" rule, which restricts browsing of the database. In this scheme, both a relatively narrowly defined user role and password protocol limits information access to "need to know," and is required to open secured files. Further, only a few APHIS/WS employees have access to the entire database as required for execution of their responsibilities. Security is built into the application user interface. People are logged off for inactivity, and access to web-pages cannot be gained from outside locations. Specifically, the access path to each web page is monitored. Monitoring of use of the system of records for profiles of misuse is possible by the ISSO or her/his designees. Privacy information within records of the MIS is removed from all data reports that are made available to the public, and are offered separately on an APHIS web-site for public access, or made available by other forms of communication (mail, e-mail, facsimile) to the public. The

	public will not have access to the database from which these summaries originate.
5a. Do other systems share data or have access to data in this system? If yes, explain.	No.
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	Not applicable. There is no interface.
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	Yes. No other agencies will have direct access to the MIS, but data contained in records of the system may be shared with other agencies in the course of business and for implementing collaborative program activities and objectives. WS may routinely share data in the MIS system with agencies which: (1) collaborate with APHIS/WS in implementation and/or regulation of wildlife management activities; (2) have an interest or regulatory responsibility in animal or public health, or (3) have responsibilities for national security may request data in the MIS to be shared. Data may be shared with State or Federal government-level representatives of the Environmental Protection Agency as part of APHIS/WS' responsibility to comply with the Federal Insecticide Fungicide and Rodenticide Act (U.S. Code Title 7, Section 136i-1).
6b. How will the data be used by the agency?	Information shared with other agencies will be used to identify and verify management actions performed by APHIS/WS under funded interagency agreement(s), Memoranda of Understanding(s), and / or permits issued by the agencies. Some data provided to land management agencies, such as the Bureau of Land Management (BLM) and the Forest Service (FS), where a cooperator has a grazing allotment also require information about wildlife damage management actions performed on the agencies

	managed lands. APHIS/WS has memoranda of understandings, or other official agreements, with such agencies for the purpose of wildlife damage management on lands controlled by them and have agreed to report wildlife damage management actions to them. This consists of information about a cooperator's resources which are being protected by a APHIS/WS action. Wildlife is a publicly owned resource and is managed by both Federal and State agencies. APHIS/WS provides informational data to the appropriate agency to demonstrate compliance with statutes, rules, regulations, orders, or permits issued by the agency. Examples include APHIS/WS activities that involve Federal and State managed and regulated wildlife species. Data concerning the locations where APHIS/WS management actions occurred can be used by the agency to improve overall management of the species. Information shared with other federal agencies may be used to monitor wildlife population health, human health, wildlife disease outbreaks, or potential national security issues related to the release or propagation of wildlife diseases which may be zoonoses for human populations, or diseases which may threaten food supplies of the United States. Information is provided to the EPA, and their agents in each State, regarding where registered pesticides are applied pursuant to APHIS/WS wildlife damage management programs. This data sharing documents compliance with the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) (U.S. Code Title 7, Section 136i-1). EPA uses this information to fulfill its federal reporting requirements under FIFRA.
6c. Who is responsible for assuring proper use of the data?	APHIS/WS is responsible for the protection and proper use of the data within the MIS. APHIS/WS restricts access to data by other agencies based on a “need to know” rule for the agency, the office or program of the agency, and the identity of the individual who receives the data. An agency’s need to know is established through interagency agreement(s), Memoranda of Understanding(s), statute(s), rule(s), regulation(s), or order(s) issued pursuant thereto. Furthermore, release of data is pursuant to the uses identified within the Privacy Act and the routine uses identified by APHIS/WS for the records maintained in the

	MIS. APHIS/WS releases the data with the understanding that the other agencies are bound by the regulations of the Privacy Act through which the data was originally released. Once this information is conveyed to representatives of the other agencies, APHIS/WS assumes no further responsibility, but documents a record of custody which identifies the office of the agency, and individual, which received the data.

ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	Yes. The information collection system being designed by APHIS/WS is for the purpose of maintaining a record of activities conducted by the agency pursuant to its mission and responsibilities authorized by the Act of 1931 (as amended), sometimes referred to as the Animal Damage Control Act of 1931. Within this area of responsibility, APHIS/WS provides service to governmental, public, and private sectors of the United States, and to foreign partners and cooperators regarding wildlife damage management. Use of data collected is relevant to these activities. That relevancy includes, but is not limited to: 1) Providing the agency with information for financial transactions between itself and its many cooperators, 2) Providing APHIS/WS employees who work directly with cooperators with information about the status of financial agreements with cooperators, program progress resulting from APHIS/WS activities on cooperator projects, wildlife damage to be addressed on cooperator property, nature of damage occurring, locations where damage is occurring, and losses resulting from wildlife damage, 3) Providing operational program managers with information to compile summaries of cooperator programs, determine status of wildlife damage management performed by specific APHIS/WS employees on specific cooperator programs where official duties are performed, and make determinations about assignment to cooperator projects of APHIS/WS employees under their supervision.

	4) Evaluate program activities, including assessment of the relative and specific effectiveness of APHIS/WS projects and the relative and specific satisfaction of cooperators. This may include preparing of mailing labels and pre-addressed forms to query or inform cooperators or field personnel, and to streamline and enhance program efficiency. 5) Other routine uses of the data include: (1) To cooperative State government officials, employees, or contractors, as necessary to carry out the program; and other parties engaged to assist in administering the program. Such contractors and other parties will be bound by the nondisclosure provisions of the Privacy Act. This routine use assists the agency in carrying out the program, and thus is compatible with the purpose for which the records are created and maintained; (2) To the appropriate agency, whether Federal, State, local, or foreign, charged with responsibility of investigating or prosecuting a violation of law or of enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, of any record within this system when information available indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and either arising by general statute or particular program statute, or by rule, regulation, or court order issued pursuant thereto; (3) To the Department of Justice when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or the United States, in litigation, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the purpose for which the records were collected; (4) For use in a proceeding before a court or adjudicative body before which the agency is

	authorized to appear, when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee, or the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the agency determines that use of such records is relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the court is a use of the information contained in the records that is compatible with the purpose for which the records were collected; (5) To appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; the agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, a risk of identity theft or fraud, or a risk of harm to the security or integrity of this system or other systems or programs (whether maintained by the agency or another agency or entity) that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. (6) To USDA employees or contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends or anomalies indicative of fraud, waste, or abuse. (7) To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. §§ 2904 and 2906.
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No. The system has the capability of creating previously unavailable data when aggregated as it relates to resource holdings of Cooperators. APHIS/WS collects, on a volunteer basis, information about quantities of resources owned by a Cooperator. This information could also contain unit or total values of these resources for any given year. Cumulative years of data about a

	Cooperator, when aggregated, could be used to determine average resource holdings, and if the Cooperator volunteered the value of these holdings, an average worth of the Cooperator's resources which APHIS/WS protects could be derived. However, no such usage of this data is made by any implemented data compilation or analysis conducted as a business practice by APHIS/WS. In addition, any aggregation processes of such information by APHIS/WS business process drops all identity as to whom those resources belong. Aggregated data is generated in APHIS/WS district, state, regional, and national reports but no connection to owners of the resources appears in those reports.
2b. Will the new data be placed in the individual's record (customer or employee)?	**Not applicable**
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	No
2d. How will the new data be verified for relevance and accuracy?	Data validation for integrity and reliability is performed by the employees entering the data, by data technicians compiling data, and by managers reviewing work performed by personnel.
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	Data consolidation is an in-house initiative in the APHIS/WS system of records until it is consolidated in the national archive as a storage process by NITC. Individuals involved in all processes are restricted to data that they are authorized to handle and the data is not exposed to any unauthorized users during this process. Standard safeguards approved by USDA for data security are used by NITC to reduce the likelihood of unauthorized access or use. Controls to protect data from unauthorized access include unique user identification, password authentication, agency implemented cybersecurity measures and firewalls installed at each access terminal, current virus protection programs updated in accordance with agency requirements and immediate lockout capability if a user is disqualified from access to data at any level. All transfer of data occurs through the agency

	standard virtual private network in encrypted formats. Hard copy components of the system are segregated and protected in secured and locked storage cabinets accessible only to authorized users. Other internal safeguards include monitoring of data management and development processes by the ISSM and ISSOs, and supervisory controls for field level data entry and handling activities.
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	The only process consolidation occurring in the system is that formerly manual processes for entering data have been converted to electronic entry techniques. In this change, processors will remain the same and steps for data entry and creating a record will remain the same. Access controls discussed in 3a serve to prevent data from unauthorized access. Control of access to data has improved and no unauthorized access of data as a result of this change has occurred or is expected. Security is built into the application user interface. People are logged off for inactivity, and access to web-pages cannot come from outside sources. That is, the access path to each web-page is monitored.
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	Yes. Under this system, data may be retrieved according to the APHIS least privilege rule which provides limited access based on the need-to-know. Retrieval is determined by the structure inherent in the database and the controls in place in the system. In this structure and under APHIS/WS established controls, data is organized by an agreement number unique to the cooperator entity, and employees can access information about the cooperator which is in the system by that unique agreement number or by the cooperator's name. Retrieval of data can take place when APHIS/WS employees previously approved and having authorization to retrieve specific data sets make a request to the server for retrieval of that information.
4b. What are the potential effects on the due process rights of customers and employees of: • consolidation and linkage of files and systems; • derivation of data • accelerated information	The following potential effects to due process of contributors related to elements of concern listed to the left are: a) Individuals (both customers and employees) could challenge any inaccuracies in the system files. b) If inaccuracies occur in the system of records and were disclosed, they could impose a liability on the agency or its employees.

processing and decision making; • use of new technologies.	c) If unnecessary disclosure of customer identity were to occur, it could subject the customer to harassment by protesters or activists. d) If recordkeeping has inaccuracies, such as reports of overdue balances, customers may have credit rating harmed as a result, especially if such information was provided to credit bureaus in cases of non-payment by a customer. Further, such action proceeding from such an error could result in impacts such as actions related to federal tax overpayment or liens on real property. e) Records may implicate APHIS/WS employees as liable for intentional or willful acts (conduct which requires more than gross negligence and amount to at least reckless behavior). f) In instances where the system of records contains information about wildlife damage experienced by a customer, or damage to humans or property by APHIS/WS actions, that record could affect indemnification or insurance settlements positively or negatively. The record might also affect appraisals on real property or personalty, or both, either positively or negatively, where wildlife damage or damage by APHIS/WS actions occurred. g) Derivation of data could infringe on the privacy rights of third parties. Such instances could occur if individuals protected by the Privacy Act were involved in actions by APHIS/WS which were performed for a customer. Example: In instances where APHIS/WS assists the U.S. Fish and Wildlife Service (USFWS) to address damage being caused by, or to, endangered species, third parties' information could sometimes be revealed as APHIS/WS provides information to USFWS under "routine uses." h) Use of new technologies: APHIS/WS contemplates implementation of electronic signature technology in the future as part of the system of records. When this occurs, effects on due process of data contributors could occur if electronically submitted signatures on cooperative agreements were misused. In addition, electronically submitted social security numbers could be susceptible to hackers and electronic submission of consent or financial forms without failsafe encryption could be subject to theft, misuse, or abuse. Hacking of cooperative agreement identification numbers might also occur by guesswork. Misplaced or stolen PIN identifiers or computers might cause information to be made accessible to unauthorized entities, as could industrial espionage resulting in stolen

	data. Computer viruses, spamming through civil disobedience, computer crashes, or power outages might corrupt or cause the loss of data. Better and timelier service to customers is one effect on due process of data contributors as a result of the use of new technologies. More efficient execution of data handling duties by employees occurs as a result of the use of new technologies.
4c. How are the effects to be mitigated?	Effects of negative impacts to data contributors is mitigated through the following procedures/strategies: a) Monitoring of usage pathways and usage patterns b) Use of locked systems c) Use of locked paper components (locked filing cabinets inside locked offices) d) virtual private network access only for remote connections to the system e) Existence of the APHIS wide area network firewall to exclude unauthorized access to electronic files f) Limited access to users based on need-to-know access g) Standard enforced APHIS and APHIS/WS cyber security policy and procedure h) Tiered access according to data usage roles

MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	**System Location and Business Practices and Implications for Consistency of Use:** The system is kept on on-line disk storage and the MIS database. Documents which are executed originals requiring signatures reside in the State or Regional APHIS/WS offices. All data locations are protected by standard safe-keeping procedures and use of that data is monitored by program and office supervisors and the system manager's assigns. Collection and use of the data is consistent throughout the program. Because of standardized collection and use practices and policies, uniform treatment of all individual contributors and contributor groups is maintained. APHIS/WS does not foresee any problems with disparity in treatment. **Data Retention Schedules and Implications for Equitable Treatment of Contributors:** Federal and State employee information is kept active in the system as long as the individual continues to work for APHIS/WS. Information identifying

	cooperators is kept in the system as long as a cooperator retains an active agreement with APHIS/WS. Upon termination of employment or lapse of an active agreement, information is archived by fiscal year for 15 years. **Data Elimination Procedures and Implications for Equitable Treatment of Contributors:** Data elimination procedures are in accordance with National Archives and Records Administration (NARA) and existing APHIS policy, and reference to these authorities for guidance is made in the APHIS/WS Information and Data Management Handbook.
2a. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	The system is kept on on-line disk storage and the MIS database. Documents which are executed originals requiring signatures reside in the State or Regional APHIS/WS offices. All data locations are protected by standard safe-keeping procedures and use of that data is monitored by program and office supervisors and the ISSM or her/his assigns. Use of the data is consistent throughout the program. The electronic component of the system of records is deposited directly into a centralized application and housed behind the OCIO firewall at NITC in Kansas City, MO. Training on how to use MIS, how to make entries and develop and process records, basic desktop and / or laptop computer, and e-mail is provided. Managers throughout the organization monitor use of the system, providing guidance or referral for new and refresher training for remote employees making use of the system of records. Data Technicians have defined roles in data integrity, management, validation, security, support, and processing policies and strategies which enhance the overall functionality and integrity of the system. All employees receive training in security and proper use of government equipment.
2b. Explain any possibility of disparate treatment of individuals or groups.	The system is a program-specific data resource for wildlife damage management, non-time and attendance tracking, and non- performance assessing. Uniform treatment of all individual contributors and contributor groups will be maintained. APHIS/WS does not foresee any problems with disparity in treatment.
2c. What are the retention periods of data in this system?	Employee information is kept active in the system as long as the individual continues to work for APHIS/WS. Information identifying cooperators is kept in the system as long as a cooperator retains an active agreement with APHIS/WS. Upon termination of employment or lapse of an active agreement, information about

	employees or cooperators is retained in accordance with retention schedules outlined in the APHIS Records Management Handbook (2003) which states that: a) temporary records of originating offices will be destroyed when three years old, and all other offices will destroy such records when two years old; b) except wildlife damage control program general correspondence records which will be destroyed at 5 years by originating offices and 3 years of age at all other offices; c) records that are permanent in nature located at the originating office, which includes case files related to mechanical and chemical control shall be transferred to the Federal Records Center (FRC) at 5 years and to NARA when 15 years old. Such records at other offices shall be destroyed when 3 years old; d) records from originating offices about Endangered Species/Section 7 Consultation case files pertaining to specific consultations, or records about wildlife damage to agricultural crops, livestock, human health and safety, nuisances, natural resources or industrial will be retired to FRC when 15 years old and to NARA when 20 years old; such records at other offices shall be destroyed at 3 years old;
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	Procedures for elimination of data at the end of retention periods are performed in accordance with data elimination procedures defined in NARA data elimination guidelines (2007), the APHIS Records Management Handbook (2003) and the APHIS/WS IDMH (2004). Procedures are documented at the APHIS/WS ITSC, Ft. Collins, CO. and available by requesting them in writing to: USDA-APHIS-WS, Operational Support Staff, 4700 River Road, Unit 87, Rm. 2D-07.3, Riverdale, MD, 20737-1234. Procedures will include using data wiping industry-standard software using 3 or more erasure passes on storage devices that will be used again. Media to be discarded, such as inoperable disk drives, compact disks, DVDs, or tapes will be destroyed.
2e. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	Agreements which keep cooperator data active are dated and renewed at or near the expiration date, at which time cooperator representatives have opportunity to update their information. This insures routine validation of information about this contributor group. In addition, data about cooperators is kept accurate and relevant by routine and frequent contact with a cooperator representative by the APHIS/WS field employee servicing the project about which the data was gathered. APHIS/WS employees access the system to perform data entry at least weekly and have opportunity to verify accuracy and relevance of most data about themselves at that time. In addition, they are prompted by the system administrator, at least quarterly, to verify their user profile information. These procedures ensure accuracy, relevance and timeliness of employee data.

	Once the data has been in the system for no more than one week, the records are "locked." In the "locked" status, records may be edited only after selecting "edit" on the screen. At that point an audit trail is engaged which shows who requested the change and why (the employee, their supervisor, etc.) If a record is changed, the person who made the change is recorded. Only certain personnel have authority to change records other than their own. Data is assumed correct unless specifically rejected (e.g. edited). Any time, up until the Program Data Reports are recorded for the public, changes may be made to records. Once the Program Data Reports are published, all records making up the summary information are locked. Change after that point will need to be mandated by Headquarters.
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	No.
3b. How does the use of this technology affect customer/employee privacy?	Not applicable.
4a. Will this system provide the capability to identify, locate, and monitor <u>individuals</u>? If yes, explain.	Yes. The system contains the names, addresses, and telephone numbers of WS customers. Using this information, these customers can be identified and located to the extent of activities outlined in the cooperative agreement. However, live monitoring or personalized tracking is not possible or appropriate for this system.
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	No.
4c. What controls will be used to	Security is built into the application user interface. Evaluation of use profiles of the system ensure that users cannot seek to locate or identify individuals without authorization, and that no attempt

prevent unauthorized monitoring?	at monitoring can occur.
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	USDA-APHIS-9 Wildlife Services – Management Information System (MIS) USDA/APHIS
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	No. The SOR is in the clearance process. After which, it will be submitted for publication in the Federal Register.

References

APHIS (Animal and Plant Health Inspection Service. 2007. APHIS Directive 3140.5. APHIS Information Systems Security (ISS) Roles and Responsibilities. http://www.aphis.usda.gov/library/directives/pdf/3140_5.pdf

________2003. APHIS Records Management Handbook. Linda Mudd, USDA, APHIS, ABS, FIRM, 4700 River Road, Unit 103, Riverdale, MD 20737.

NARA (National Archives and Records Administration). 2007. Records Scheduling and Disposition. http://www.archives.gov/records-mgmt/faqs/scheduling.html

APHIS/WS (Wildlife Services). 2004. Information and Data Management Handbook. APHIS, Wildlife Services, Operational Support Staff, 4700 River Road, Unit 87, Rm. 2D-07.3, Riverdale, MD, 20737-1234.

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the **Wildlife Services, Management Information System (MIS)**. This document has been completed in accordance with the requirements of the E-Government Act of 2002.

MANAGEMENT CERTIFICATION – Please check the appropriate statement.

___X___ The document is accepted.

________ The document is accepted pending the changes noted.

________ The document is not accepted.

____ **We** fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

System Manager — DATE

OCIO/Project Representative — DATE

Program/Office Head — DATE

OCIO — DATE

Tammi S Hies — 12/7/07

Chief FOI/PA — DATE

Tammi S Hies — 12/7/07

Senior Official for Privacy — DATE